Weekly Cyber Risk Roundup: Payment Card Breaches, Encryption Debate, and Breach Notification Laws

by Jeff Peters on March 10, 2018

of sale breach at Applebee's restaurants that affected 167 locations across 15 states.

The malware, which was discovered on February 13, 2018, was “designed to capture payment card information and may have affected a limited number of purchases” made at Applebee’s locations owned by RMH Franchise Holdings, the company said in a statement.

News outlets reported many of the affected locations had their systems infected between early December 2017 and early January 2018. Applebee’s has close to 2,000 locations around the world and 167 of them were affected by the incident.

In addition to Applebees, MenuDrive issued a breach notification to merchants saying that its desktop ordering site was injected with malware designed to capture payment card information. The incident impacted certain transactions from November 5, 2017 to November 28, 2017.

“We have learned that the malware was contained to ONLY the Desktop ordering site of the version that you are using and certain payment gateways,” the company wrote. “Thus, this incident was contained to a part of our system and did NOT impact the Mobile ordering site or any other MenuDrive versions.”

Finally, there is yet another breach notification related to Sabre Hospitality Solutions’ SynXis Central Reservations System — this time affecting Preferred Hotels & Resorts. Sabre said that a unauthorized individual used compromised user credentials to view reservation information, including payment card information, for a subset of hotel reservations that Sabre processed on behalf of the company between June 2016 and November 2017.

The Poisoning of Col. Sergei Skripal: Russian Retribution?

Splunk to Dive Deeper into Cybersecurity with Phantom Buy

Stealing Infrastructure: Cryptomining Attacks on Container Environments

Exim Flaw Puts Hundreds of Thousands of Email Servers at Risk

Splunk to Dive Deeper into Cybersecurity with Phantom Buy

×

Upcoming Webinars »

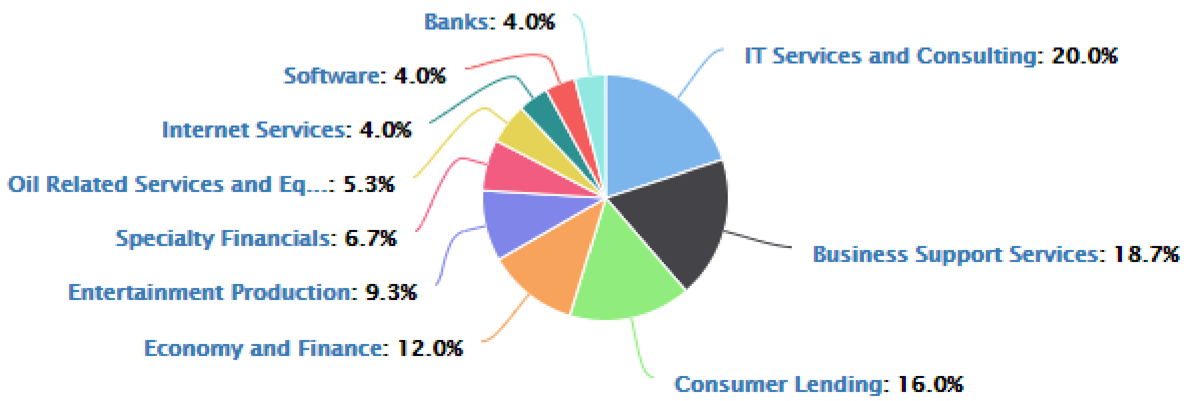
APR 02 **RSA 2018- What’s Hot in the Cyber Security Space**

April 2 @ 1:00 pm - 2:00 pm

Security Boulevard Chats

Cloud, DevSecOps and Network Security, All Together? February 26, 2018

Security-as-Code with Tim Jefferson, Barracuda Networks January 19, 2018



Other trending cybercrime events from the week include:

- **Marijuana businesses targeted:** MJ Freeway Business Solutions, which provides business management software to cannabis dispensaries, is notifying customers of unauthorized access to its systems that may have led to personal information being stolen. The Canadian medical marijuana delivery service JJ Meds said that it received an extortion threat demanding $1,000 in bitcoin in order to prevent a leak of customer information.
- **Healthcare breach notifications:** The Kansas Department for Aging and Disability Services said that the personal information of 11,000 people was improperly emailed to local contractors by a now-fired employee. Front Range Dermatology Associates announced a breach related to a now-fired employee providing patient information to a former employee. Investigators said two Florida Hospital employees stole patient records, and local news reported that 9,000 individuals may have been impacted by the theft.
- **Notable data breaches:** Ventiv Technology, which provides workers' compensation claim management software solutions, is notifying customers of a compromise of employee email accounts that were hosted on Office365 and contained personal information. Catawba County services employees had their personal information compromised due to the payroll and human resources system being infected with malware. Flexible Benefit Service Corporation said that an employee email account was compromised and used to search for wire payment information. A flaw in Nike's website allowed attackers to read server data and could have been leveraged to gain greater access to the company's systems. A researcher claimed that airline Emirates is leaking customer data.

Compass January 19, 2018

Deception: Art or Science, Ofer Israeli, Illusive Networks January 16, 2018

Tips to Secure IoT and Connected Systems w/ DigiCert November 29, 2017

Industry Spotlight »

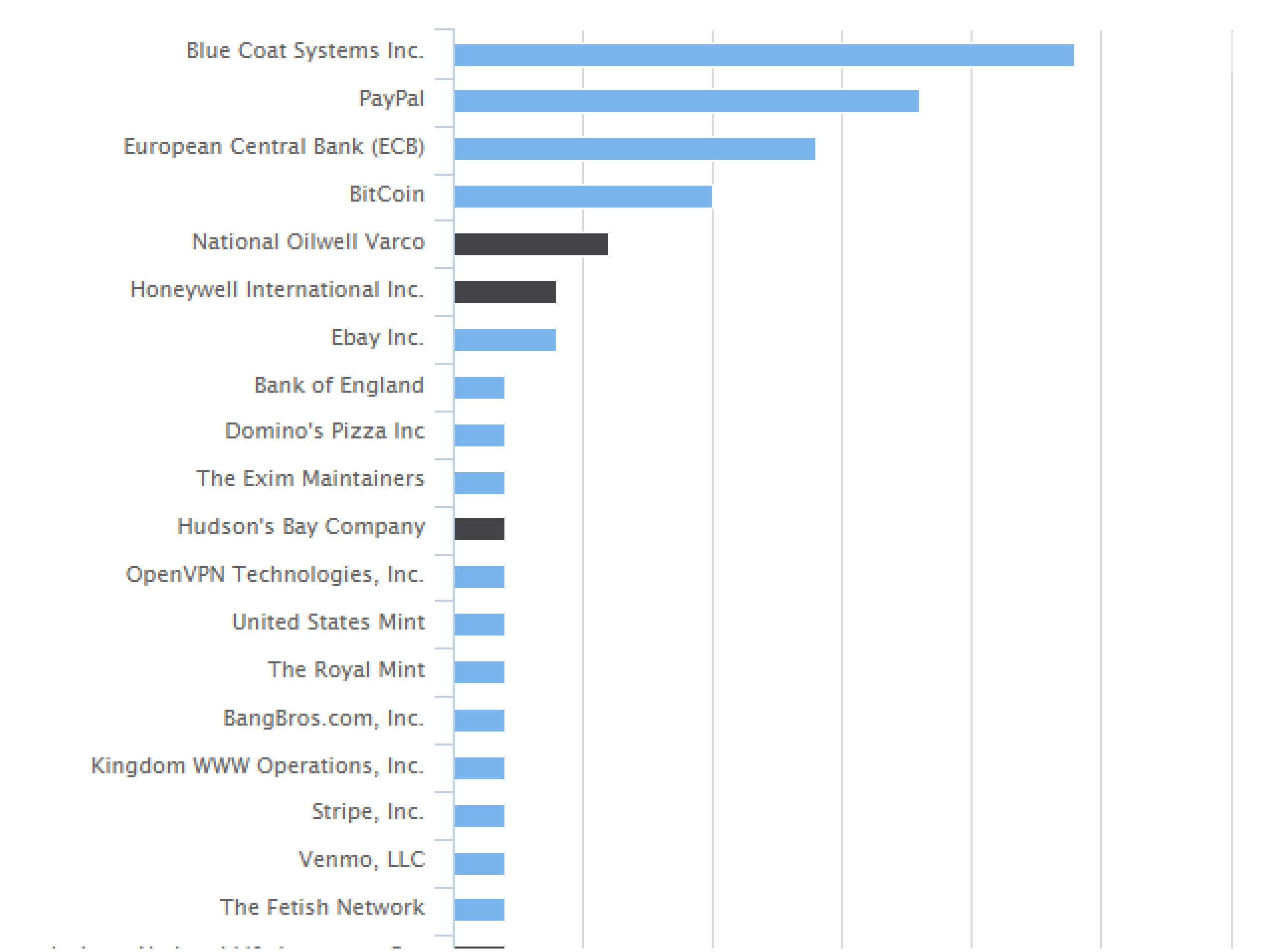
Mitigating Cyber-Risks in Everyday Technology Use

The EU GDPR Checklist: Be Aware, Be Prepared

> exchange Binance said that its users were the target of “a large scale phishing and stealing attempt” and those compromised accounts were used to perform abnormal trading activity over a short period of time. The spyware company Retina-X Studios said that it “is immediately and indefinitely halting its PhoneSheriff, TeenShield, SniperSpy and Mobile Spy products” after being “the victim of sophisticated and repeated illegal hackings.”

SurfWatch Labs collected data on many different companies tied to cybercrime over the past week. Some of the top trending targets are shown in the chart below.

Trending Cybercrime Targets

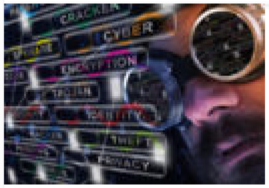


Compliance and GDPR

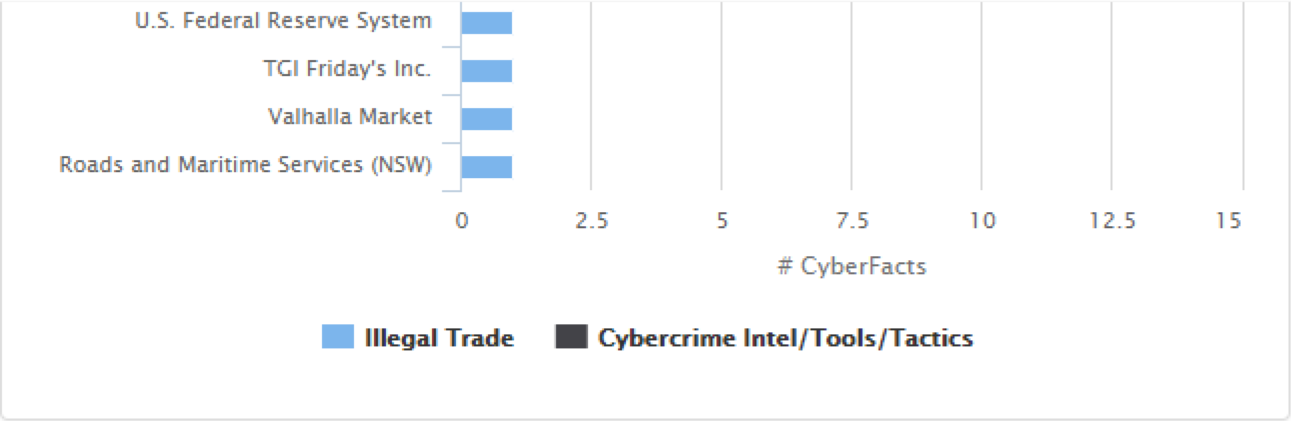
Top Stories »

Splunk to Dive Deeper into Cybersecurity with Phantom Buy

Worm Infects Redis, Windows Servers with Cryptomining Malware

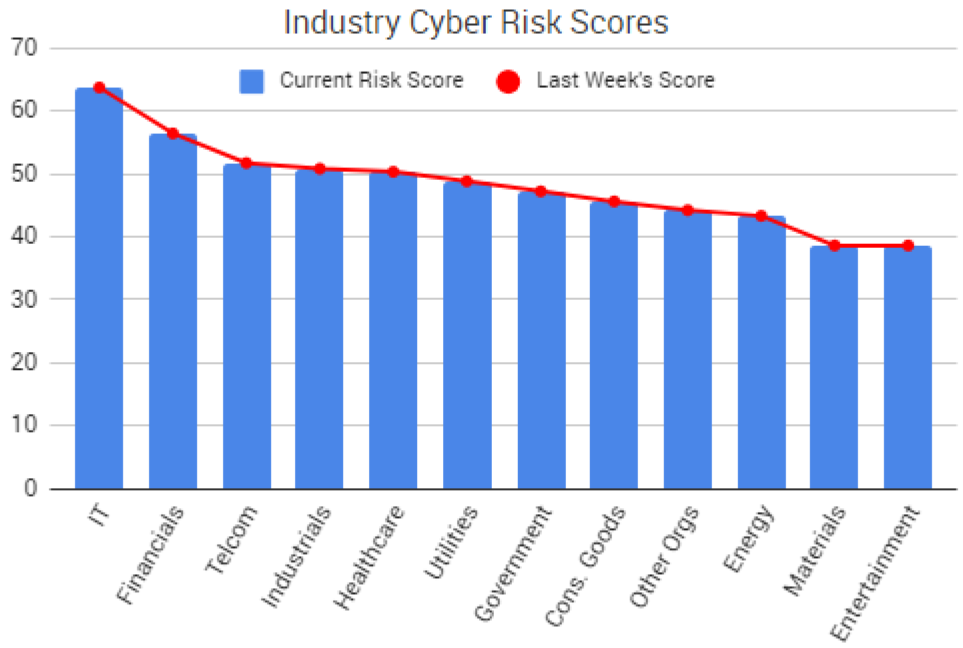


Exim Flaw Puts Hundreds of Thousands of Email Servers at Risk



Cyber Risk Trends From the Past Week

There were several regulatory stories that made headlines this week, including the FBI's continued push for a stronger partnership with the private sector when it comes to encryption, allegations that Geek Squad techs act as FBI spies, and new data breach notification laws.



that there were 7,775 devices that the FBI could not access due to encryption in fiscal 2017, despite having approval from a judge. According to Fry, that meant the FBI could not access more than half of the devices they tried to access during the period.

“Let me be clear: the FBI supports information security measures, including strong encryption,” Fry said. “Actually, the FBI is on the front line fighting cyber crime and economic espionage. But information security programs need to be thoughtfully designed so they don’t undermine the lawful tools we need to keep the American people safe.”

However, Ars Technica noted that a consensus of technical experts has said that what the FBI has asked for is impossible.

In addition, the Electronic Frontier Foundation obtained documents via a Freedom of Information Act lawsuit that revealed the FBI and Best Buy’s Geek Squad have been working together for decades. In some cases Geek Squad techs were paid as much as $1,000 to be informants, which the EFF argued was a violation of Fourth Amendment rights as the computer searches were not authorized by their owners.

Finally, the Alabama senate unanimously passed the Alabama Breach Notification Act, and the bill will now move to the house.

“Alabama is one of two states that doesn’t have a data breach notification law,” said state Senator Arthur Orr, who sponsored Alabama’s bill. “In the case of a breach, businesses and organizations, including state government, are under no obligation to tell a person their information may have been compromised.”

With both Alabama and South Dakota recently introducing data breach notification legislation, every resident of the U.S. may soon be protected by a state breach notification law.

- Weekly Cyber Risk Roundup: Record-Setting DDoS Attacks, Data Breach Costs
- Weekly Cyber Risk Roundup: W-2 Theft, BEC Scams, and SEC Guidance
- Weekly Cyber Risk Roundup: Olympic Malware and Russian Cybercrime

More from Jeff Peters

Share this:

2 More

Related

Point-of-Sale Breach Confirmed at Some Applebee's Locations
March 5, 2018
In "Data Security"

Sonic Investigates Breach, 5 Million Cards For Sale on Cybercriminal Market
September 27, 2017
In "Security Bloggers Network"

Weekly Cyber Risk Roundup: More Payment Card Breaches and Dark Web Arrests
November 20, 2017
In "Governance, Risk & Compliance"

This is a Security Bloggers Network syndicated blog post authored by Jeff Peters. Read the original post at: SurfWatch Labs, Inc.

Applebee's, Best Buy, encryption, point of sale, regulations, security bloggers network, Weekly Cyber Risk Roundup

← J.D. Iliad Frazer's ...ret VK Messenger (VKontakte) vk:// URI Handler Commands Execution →

Security Boulevard Comment Policy

Comments are moderated

0 Comments **Security Boulevard** 1 **Login**

♡ **Recommend** **Share** **Sort by Best**

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

ALSO ON **SECURITY BOULEVARD**

Five Cloud Migration Strategies for Applications

1 comment • 2 months ago

hel — Or, directly migrate data from original cloud to target cloud with cloud migration tool just like described

Six Requirements for Achieving DevSecOps

1 comment • 20 days ago

Mark Hermeling — Great discussion, nice and broad to set up the field.Re your statement:Documented CVEs: Weaknesses in

1 comment • a month ago

Raffael Marty — I definitely agree with you on the contextual visualizations. I don't agree that game engines, or 3D for that matter, will help

2 comments • 24 days ago

DevOps.com — MichaelSome of the security bloggers network articles are only summaries, but there are links to the full article on the

✉ Subscribe   Add Disqus to your siteAdd DisqusAdd   🔒 Privacy

SECURITY

Home of the Security Bloggers Network

Join the Community

- Add your blog to Security Bloggers Network
- Write for Security Boulevard
- Bloggers Meetup and Awards
- Ask a Question
- Email: info@securityboulevard.com

Useful Links

- About
- Media Kit
- Sponsors Info
- Copyright
- TOS
- Privacy Policy

Other Mediaops Sites

- Container Journal
- DevOps.com
- DevOps Connect
- DevOps Institute